Amendments to the Specification

Please replace the paragraph beginning at page 25, line 7 with the following new paragraph:

In a second step 23 directly after step [[1]] 19, the entity A generates a first element of proof x by applying, to the message M, jointly with the number P, a function h, for example equal to a cryptographic hash function or including a cryptographic hash function, such that:

$$x = h(P,M).$$

Please replace the paragraph beginning at page 28, line 27 with the following new paragraph:

In step 2, the index [[p]] j is increased by a unitary increment so as to repeat step 45 and step 2, as long as j is detected in a transition 3, different from j' modulo k, until a transition 4 detects that j is equal to j' modulo k, in order to return to the output of step 29 after k executions of step 45.

Please replace the paragraph beginning at page 30, line 39 with the following new paragraph:

The prover device 30 includes communication means 34 and calculation means 37. The prover device 30 is protected from intrusion. The communication means 34 ~~are~~ is designed to transmit the first element of proof x, in accordance with step 9, 45 or 47, described with reference to figures 1, 3 or 4, the second element of proof y, in accordance with step 13 described with reference to figures 1 and 3, at step 24 described with reference to figure 2 or at steps 2 and 48 described with reference to figure 4, the message M, in accordance with steps 19, 20, 44 or 47 described with reference to figures 1 to 4, or the common number c, in accordance with step 24, 46 described with reference to figures 2 and 4, depending on the version of the method to be implemented. The communication means 34 ~~are~~ is also designed to receive the common number c, in accordance with the transition 12 or 1 described with reference to

figures 1 to 4, when versions of the method to be implemented correspond to identification or to authentication. For a version of the method to be implemented corresponding to a signature, the communication means 34 do not need to be designed to receive the common number c.

Please replace the paragraph beginning at page 31, line 24 with the following new paragraph:

The calculation means 37 ~~are~~ is designed to execute steps 9 and 13 described with reference to figure 1 or 5, steps 18, 19, 23 and 24 described with reference to figure 2, and steps 13 and 20 described with reference to figure 3 or the steps described with reference to figure 4, depending on the version of the method to be implemented. The calculation means 37 comprise, in a known manner, a microprocessor and microprograms or combinatory circuits dedicated to the calculations described above.

Please replace the paragraph beginning at page 31, line 35 as follows:

The verifier device 31 includes communication means 35 and calculation means 38. The communication means 35 ~~are~~ is designed to transmit one or more common numbers c, in accordance with step 11 described with reference to figures 1, 3 and 5, when versions of the method to be implemented correspond to authentication. For a version of the method to be implemented corresponding to a signature, the communication means 35 have no need to be designed to transmit the common number c. The communication means 35 ~~are~~ is also designed to receive the two elements of proof x and y, in accordance with the transitions 10 and 16 described with reference to figures 1 to 3 and 5, a message M with the first element of proof x and the second element of proof y, in accordance with the transitions 21 and 16 described with reference to figure 3, or the second element of proof and the message M with one or more common numbers c and the private key image y, in accordance with the transitions 2 and 8 described with reference to figure 5.

Please replace the paragraph beginning at page 32, line 17 with the following paragraph:

The calculation means 38 ~~are~~ is designed to execute steps 11 and 17 described with reference to figures 1 and 5, step 26 described with reference to figure 2 or steps 11 and 22 described with reference to figure 3, depending on the version of the method to be implemented. The calculation means 38 comprise, in a known manner, a microprocessor and microprograms or combinatory circuits dedicated to the calculations described above.

Please replace the paragraph beginning at page 32, line 27 with the following paragraph:

The intermediate device 32 includes communication means 36 and calculations means 39. The communication means 36 ~~are~~ is designed to transmit the third element of proof Y in accordance with step 15 described with reference to figure 5. The communication means 36 ~~are~~ is also designed to receive the second element of proof y in accordance with the transition 14 described with reference to figure 5.

Please replace the paragraph beginning at page 32, line 36 with the following paragraph:

The calculation means 39 ~~are~~ is designed to execute step 15 described with reference to figure 5. The calculation means 39 comprise, in a known manner, a microprocessor and programs or combinatory circuits dedicated to the calculations described above.